Aksika, Virus Lokal "Open Source"

Berawal dari *posting source code* virus di sebuah situs komunitas pemrograman, maka seperti yang diperkirakan, tak lama kemudian muncullah virus-virus hasil *compile* dari source code tersebut. Dan sampai saat ini virusnya pun masih menyebar.

Arief Prabowo

Sedang tren, virus yang menyerupai folder.

Apabila kita men-*download* paket *source code* dari virus Aksika ini memang tidak terdapat file *executable* hasil *compile*-an dari source code-nya. Namun hanya dengan bermodalkan source code dan program compiler nya saja, orang awam sekalipun dapat menciptakan virusnya dengan mudah atau bahkan sebelum di-compile. Bisa saja source code tersebut diubah ataupun ditambahkan rutin–rutin tertentu atau rutin jahat sekalipun sebelum disebarluaskan, yang akhirnya terciptalah varian-varian baru dari virus Aksika.

Virus yang dapat menyebar melalui berbagai media penyimpanan ini dibuat dengan menggunakan salah satu bahasa pemrograman favorit para pembuat virus-saat ini. Ya, bahasa pemrograman tersebut adalah Visual Basic 6.0.

Pada sample yang kami punya, ukuran tubuh virus ini yang sebelum di-*compress* sekitar 98 Kb, namun ada juga yang sudah di-compress menggunakan tool executable compressor seperti UPX, dan jelas ukurannya menjadi lebih kecil.

Beberapa ciri fisik dari virus ini, di antaranya ia menggunakan icon folder seperti kebanyakan virus lokal lainnya. Pada *Version Information,* akan terlihat beberapa informasi, contoh pada value Internal Name akan berisi "4K51K4". Inipun sebenarnya tergantung pada apakah virus tersebut sudah diubah atau belum, dan apabila sudah dimodifikasi mungkin akan berbeda.

Registry Key
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Logon%username%
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\System Monitoring
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\4k51k4
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MSMSGS
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Service%UserName%
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\Debugger
HKCU\Control Panel\Desktop\Scrnsave.exe
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
HKCR\exefile\shell\open\command
HKCR\lnkfile\shell\open\command
HKCR\piffile\shell\open\command
HKCR\batfile\shell\open\command
HKCR\comfile\shell\open\command

Beberapa *registry key* pemicu yang dibuat atau diinfeksi oleh Aksika agar ia dapat aktif.

Mulai Infeksi

Pada saat virus yang "menjelma" sebagai folder ini dieksekusi untuk kali pertama, mungkin tidak kelihatan adanya perubahan pada komputer Anda atau bisa saja Anda sedikit curiga dikarenakan folder yang diklik tidak kunjung terbuka. Begitu virus aktif, ia akan segera membuat file induk pada direktori Windows dengan nama 4k51k4.exe, pada direktori System32 dengan nama lexplorer.exe dan shell.exe, dan juga beberapa file induk lainnya yang ia buat pada direktori \Documents and Settings\%UserName%\Local Settings\Application Data\Windows, dengan menggunakan nama–nama yang mirip dengan program atau *services* milik Windows, seperti winlogon.exe, csrss.exe, lsass.exe, services.exe, dan lain-lain.

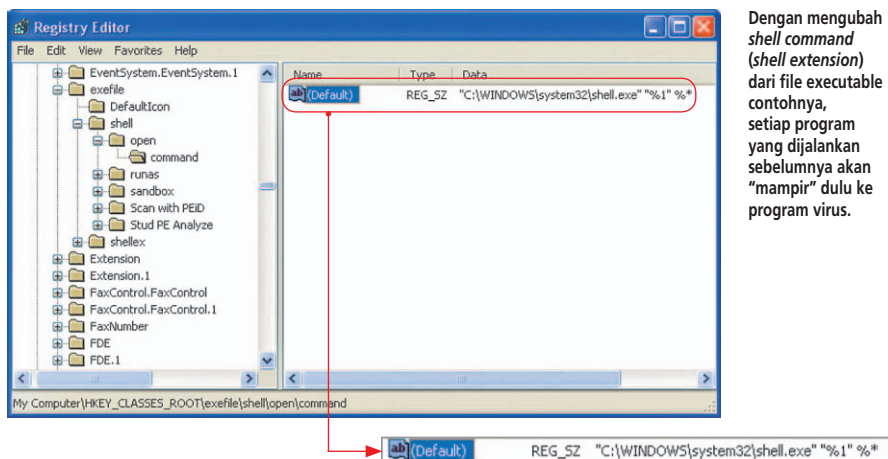
Setelah ia berhasil menanamkan file–file induk tadi, lalu baru ia akan membukakan jalan agar Windows selalu menjalankan file induk virus tersebut otomatis pada saat start Windows. Yakni, dengan jalan mengubah registry ataupun menambahkan file pada StartUp Folder.

Ia juga akan mencari setiap drive yang ada pada komputer tersebut, dan mulai menggandakan dirinya ke setiap drive yang ditemuinya. Dan juga ia akan mencoba untuk menciptakan dua buah file dengan nama desktop.ini dan folder.htt pada direktori 4K51K4, yang dimaksudkan agar virus ini otomatis dijalankan ketika user membuka folder tersebut. Namun pada *operating system* Windows XP ke atas, sepertinya fungsi ini tidak dapat berjalan.

Infeksi Registry

Virus ini memang tak tanggung–tanggung dalam melakukan serangan ke registry, karena Registry Editor, Folder Options, Task Manager, Command Prompt, dan beberapa fitur penting dari Windows lainnya juga ikut di-*disable*. Dengan bantuan registry, ia juga akan menyembunyikan extension dari setiap file dan juga mengubah Type dari file executable menjadi "File Folder". Jelas sekali tujuannya untuk mengamuflasekan diri agar dapat mempersulit *user* dalam membedakan mana yang benar-benar folder dan mana yang virus. Karena seperti yang kita ketahui bahwa virus ini memiliki icon yang menyerupai sebuah folder.

Gempuran terhadap registry tak berhenti sampai di situ saja, *shell extension* juga ikut diinfeksi. Apa yang terjadi bila ini diubah? Maka setiap file atau program yang Anda eksekusi, sebelumnya akan diarahkan pada virus ini, baru selanjutnya diteruskan ke program yang asli. Program–program yang telah dieksekusi ini selanjutnya akan disembuyikan dengan cara mengeset attribut-nya sebagai Hidden dan ReadOnly, agar tidak tampak pada Explorer, dan digantikan dengan file virus dengan nama hampir menyerupai aslinya. Yang membedakannya, yaitu nama file virus dakhiri dengan spasi.

Seperti yang kita ketahui bahwa virus yang dibuat menggunakan Visual Basic pasti membutuhkan run time library (msvbvm60.dll), tanpa file tersebut virus ini tidak akan dapat berjalan. Oleh karena itu, virus pun akan membuat *back-up* dari file msvbvm60.dll pada direktori Windows dengan mengeset attribut-nya sebagai *Hidden* dan *Read Only* kalau misalnya sewaktu–waktu file tersebut ada yang menghapusnya.

Dengan mengubah *shell command* (*shell extension*) dari file executable contohnya, setiap program yang dijalankan sebelumnya akan "mampir" dulu ke program virus.

Satu hal yang tidak kurang dari suatu virus adalah pesan–pesan dari sang empunya virus. Virus Aksika ini juga memiliki pesan yang akan ditampilkannya pada tanggal–tanggal tertentu. Pada sampel yang kami punya, ia akan menampilkan pesan tersebut pada bulan apapun setiap tanggal 1 atau 12.

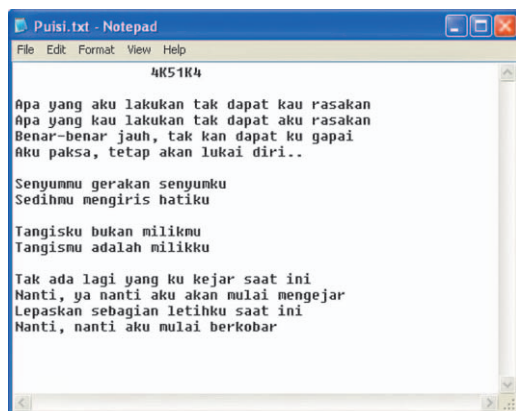
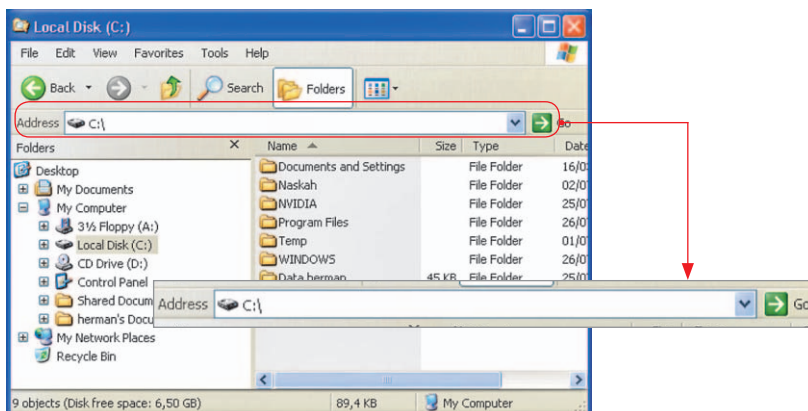
Stay Resident in Memory

Akan cukup repot untuk melumpuhkan virus ini di memory, karena *process* virus yang ada akan saling memanggil. Jadi apabila salah satu process dari virus tersebut hilang, maka "temannya" yang lain akan saling memanggil lagi.

Begitu aktif di memory, secara *real time* akan terus memonitor program–program apa saja yang dijalankan oleh user. Saat Windows Explorer aktif, virus ini akan membaca *string path* yang ada pada Address Bar dari Windows Explorer untuk mendapatkan direktori aktif, lalu membuat duplikat dirinya sendiri pada direktori tersebut dengan menggunakan nama yang sama.

Tak hanya itu saja, dengan berpatokan pada string path tadi, ia juga akan mencari file–file dengan *extension* tertentu, seperti .mp3, .mpg, jpg, dan lain-lain. Apabila ditemukan, file tersebut akan diset attribut-nya menjadi hidden dan read only dan digantikan dengan file virus.

Seperti yang dilakukan oleh pendahulunya, Brontok, ia juga akan membaca *captions* setiap program, apabila masuk dalam kriteria program pengganggu menurut sang virus, maka Windows akan di-*restart*. Program–prog ram yang masuk ke dalam kriteria penggangu menurut Aksika adalah program–program yang pada caption-nya terdapat beberapa kata, seperti ANT, VIR, TASK, ASM, REG, ASM, W32, BUG, DBG, HEX, DETEC, PROC, WALK, REST, AVS, dan OPTIONS.

Kami telah meng-*update* PCMAV agar dapat membasmi virus ini. Apabila komputer Anda terinfeksi, silakan scan menggunakan PCMAV RC7 ini. Namun, apabila ternyata PCMAV tidak bisa mendeteksi virus Aksika yang menyerang komputer Anda, silakan Anda kirimkan sampelnya kepada kami. Kami tunggu! ■

Pesan dari sang empunya virus.

Membaca *Address Bar* dari Windows Explorer untuk mendapatkan direktori aktif.